FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1320646-0

Total Deleted Page(s) = 13
Page 4 ~ Duplicate;
Page 5 ~ Duplicate;
Page 6 ~ Duplicate;
Page 7 ~ Duplicate;
Page 11 ~ Referral/Consult;
Page 12 ~ Referral/Consult;
Page 13 ~ Referral/Consult;
Page 14 ~ Referral/Consult;
Page 15 ~ Referral/Consult;
Page 16 ~ Referral/Consult;
Page 17 ~ Referral/Consult;
Page 18 ~ Referral/Consult;
Page 19 ~ Referral/Consult;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

NIPC

Computer Investigations Unit

#11
FBI

to: CITA Supervisor FG

fax#: 404-679-6296

re: Electronic Disturbance Theater (EDT)

date: 11/13/98

pages: (8)

comments: This group is threatening to launch an electronic attack against the School of America, Fort Benning, Georgia, on 11/22/98.

Thanks,

[redacted]
eqf 0328

SA [redacted]

1. Announced in DIA communication; Bu EC enroute.
2. FBIHQ (Ms. [redacted]) recommends coordination w/ NYO + WFO
3. I have given a heads up to CID at Ft Gillem. POCs — SA [redacted] SA [redacted] or SA [redacted]
4. Pls designate a case agent & have him/her OPA a case.

b6
b7C

FG 11/13/98

11/18/98
OPA [redacted]

SA [redacted]

[redacted] keep me posted. [redacted]

288-AT-87255-1

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/04/1998

To: New York

From: New York

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288-NY-268557 b6 b7C

Title: Electronic Disturbance Theater;
[redacted]
CITA
OO:NY

Synopsis: Request case to be opened and assigned to SA [redacted]

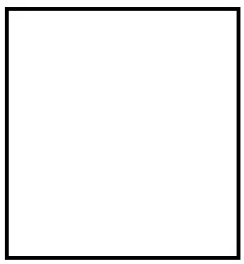
Details: Case is predicated upon information provided by AUSA [redacted] Eastern District of Virginia. b6 b7C Subject Electronic Disturbance Theater (EDT) is a group claiming on its Internet website to protest various national and international policies through orchestrated attacks on computer systems. The attacks employ a program called "FloodNet" which causes a denial of service to the target computer. EDT's Internet website solicits visitors to participate in coordinated attacks of a computer system chosen by EDT. Participants simply click on the FloodNet icon on the EDT's website at a predetermined and published date and time. This icon then initiates a Java applet which repeatedly reloads files from a victim's computer system at a unusually high rate. This activity, when multiplied by many users, will cause service interruptions and possibly crash the server computer unless early detection is made and countermeasures are implemented. The visitors do not control the destination of the attack, rather it is programed into the applet on the EDT's website.

The EDT claims that it designed the FloodNet program and has attacked computer systems owned by the government of Mexico, the Department of Defense and the German Stock Exchange.

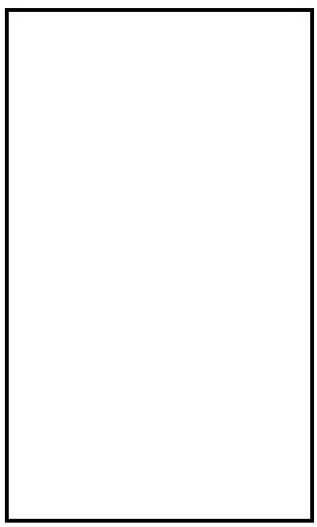
The following proprietors of EDT are believed to be New York University Graduate students located in New York, New York:

Descriptive Data:

Main Subject
Name -
Last:
First:
Race:
Sex:
DOB:
SOC:
SOC:

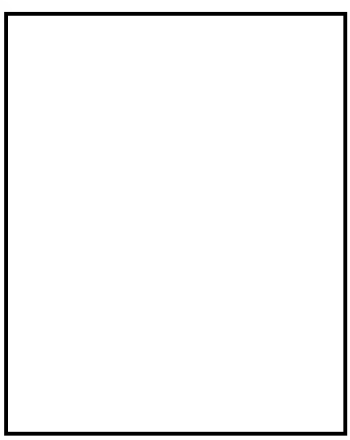


Main Subject
Name -
Last:
First:
Middle:
Race:
Sex:
DOB:
POB:
Address -
House #:
Street Name:
Unit:
City:
State:
Postal Code:



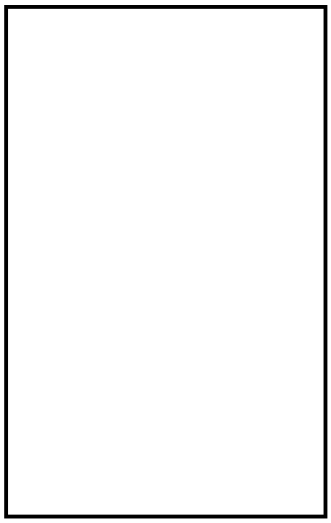
b6
b7C

Main Subject
Name -
Last:
First:
Race:
Sex:
DOB:
Address -
House #:
Street Name:
City:
State:
Postal Code:
Phone:



To: New York From: New York
Re: 288-NY-, 11/04/1998

Main Subject
Name -
Last:
First:
Middle:
Race:
Sex:
DOB:
Address -
House #:
Street Name:
Unit:
City:
State:
Postal Code:
Phone:



b6
b7C

♦♦

0005 MRI 00522/327

PP FBIAT FBINY FBIWF

DE RUCNFB #0025 3271903

ZNY EEEEE

P 231811Z NOV 98

FM DIRECTOR FBI (288-NY-268557)

TO ZEN/AFIWC KELLY AFB TX//DO/IOC///PRIORITY/

ZEN/HQ AFOSI XOQ BOLLING AFB DC//XOII///PRIORITY/

ZEN/AFOC WASHINGTON DC/PRIORITY/

ZEN/CIA WASHINGTON DC//DDO CTC/C/OAG/EC/CCB/CTC///PRIORITY/

ZEN/CDRMDW FT MCNAIR WASHINGTON DC//ANOP///PRIORITY/

ZEN/CDRUSACIDC FT BELVOIR VA//CIOP-IN///PRIORITY/

ZEN/CINCUSACOM NORFOLK VA//CDO/J33///PRIORITY/

ZEN/DA WASHINGTON DC//DAMO-AOC/DAMO-ODL-FP/DAMI-CH/DAMI-POD///PRIORITY/

ZEN/DIRACIC FT GEORGE G MEADE MD//IAMG-C-ACIC///PRIORITY/

ZEN/DISA WASHINGTON DC//D16/D312/D3332///PRIORITY/

ZEN/DEPT OF JUSTICE WASHINGTON DC/PRIORITY/

ZEN/DEPT OF JUSTICE COMMAND CENTER WASHINGTON DC/PRIORITY/

ZEN/DIA WASHINGTON DC//TERR DESK/TWC-2///PRIORITY/

ZEN/DIR LIWA FT BELVOIR VA/PRIORITY/

ZEN/117PLA//HQ AIA DIR OF OPERATIONS KELLY AFB TX/IOC///PRIORITY/

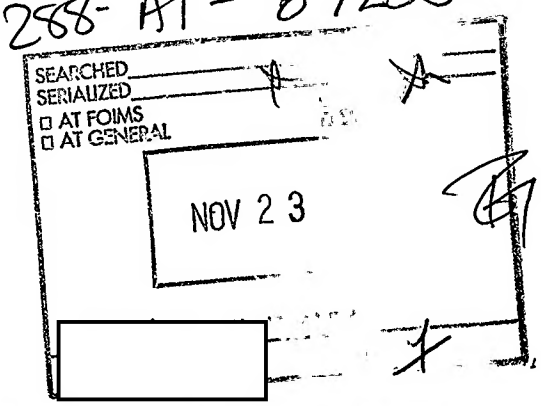
1. SA [redacted]

2. SA [redacted]

3 [redacted]

b6
b7C

288-AT-872553



PAGE TWO DE RUCNFB 0025 UNCLAS E F T O

ZEN/JOINT STAFF WASHINGTON DC//J2MI/J3/J33/J34/J39/J6K/NMCC///PRIORITY/

ZEN/DIRNSA FT GEORGE G MEADE MD//NSOC/SIPO/IPA///PRIORITY/

ZEN/SECDEF WASHINGTON DC//C3I/USDA:SO-LIC///PRIORITY/

ZEN/USCINCSO MIAMI FL//JOIC///PRIORITY/

ZEN/WHITE HOUSE NATIONAL SECURITY COUNCIL WASHINGTON DC/PRIORITY/

ZEN/WHITE HOUSE SITUATION ROOM WASHINGTON DC/PRIORITY/

FBI ATLANTA/PRIORITY/

FBI NEW YORK/PRIORITY/

FBI WASHINGTON FIELD/PRIORITY/

INFO ZEN/117PLA//DEFINTEL AGENCY SAFE READD WASHDC///PRIORITY/

BT

UNCLAS E F T O

CITE: //1332//

PASS: DISA PLEASE PASS TO APPROPRIATE DOD FACILITIES; NSA FOR ZKZK PP ZSL DE; WHITE HOUSE SITUATION ROOM PLEASE PASS TO EOP SECURITY OFFICE.

SUBJECT: NIPC COMPUTER INTRUSION ALERT: ALLEGED ACTS OF ELECTRONIC DISRUPTION TO TARGET THE U.S. ARMY'S SCHOOL OF THE AMERICAS (SOA) ON NOVEMBER 22.

REFERENCE: DIRECTOR FBI WASHINGTON DC 090305Z SEP 98 (NOTAL), CAPTIONED QUOTE ALLEGED ACTS OF ELECTRONIC DISRUPTION TO TARGET

CERTAIN U.S., MEXICAN, AND GERMAN INTERNET-BASED SITES AND SERVICES, SEPTEMBER 9 THROUGH NOVEMBER 22, 1998, IN SYMPATHY WITH ZAPATISTA MOVEMENT UNQUOTE.

WARNING NOTICE: ALTHOUGH UNCLASSIFIED, THIS COMMUNICATION SHOULD NOT BE FURNISHED TO THE MEDIA OR OTHER AGENCIES OUTSIDE THE LAW ENFORCEMENT/U.S. GOVERNMENT COMMUNITY WITHOUT THE PERMISSION OF THE FBI/NIPC. UNAUTHORIZED DISCLOSURE OF FBI COMMUNICATIONS COULD JEOPARDIZE ONGOING FBI INVESTIGATIONS.

1. AN ENTITY KNOWN AS THE QUOTE ELECTRONIC DISTURBANCE THEATER UNQUOTE (EDT), SYMPATHETIC TO THE ZAPATISTA MOVEMENT, HAS BEEN CALLING FOR CIVIL DISOBEDIENCE ACTION AT THE SCHOOL OF AMERICAS ON NOVEMBER 22. THIS IS THE LATEST ROUND OF ACTIONS CARRIED ON THE EDT'S PUBLICLY-ACCESSIBLE WEB SITE (HTTP://WWW.THING.NET/ (TILDE) RDOM/ECD/NOVEMBER22.HTML). THE EDT CLAIMS ITS ACTIONS HAV BEEN PROMPTED BY THE SCHOOL'S INCREASING ROLE IN TRAINING T4E MEXICAN MILITARY SINCE THE JANUARY 1, 1994, ZAPATISTA UPRISING. THE EDT IS A GROUP CONSISTING OF ACTIVISTS WHO HAVE PRIMARILY TARGETED U.S. AND MEXICAN GOVERNMENT SITES IN SUPPORT OF MEXICO'S ZAPATISTA NATIONAL LIBERATION ARMY (EZLN).

2. THE EDT HAS A HISTORY OF CARRYING OUT ITS THREATS UTILIZING

FLOODNET, A DENIAL-OF-SERVICE SOFTWARE TOOL, DESIGNED TO DISRUPT ACCESS TO TARGETED WEB SITES BY FLOODING THE HOST SERVER WITH REPEATED REQUESTS FOR THAT WEB PAGE. TO ACCOMPLISH THIS, FLOODNET USERS SIMPLY LEAVE THEIR BROWSERS OPEN, WHICH ALLOWS THE FLOODNET APPLET TO AUTOMATICALLY RELOAD A TARGET WEB PAGE EVERY FEW SECONDS. THIS TOOL ALSO ALLOWS THE USER TO POST HIS OWN MESSAGES ON THE TARGET WEB PAGE.

3. ON SEPTEMBER 9, 1998 THE EDT MOUNTED AN UNSUCCESSFUL ATTACK ON A DOD WEB SITE USING FLOODNET. ON OCTOBER 5, 1998, THE GROUP SPONSORED A DEMONSTRATION OUTSIDE THE FEDERAL COMMUNICATIONS COMMISSION (FCC) HEADQUARTERS BUILDING IN WASHINGTON D.C. THE GROUP STATED THAT IT WAS QUOTE PROTESTING THE FCC'S ROLE IN SUPPRESSING FREE SPEECH ON THE AIRWAVES UNQUOTE.

4. NATIONAL INFRASTRUCTURE PROTECTION CENTER (NIPC) COMMENT: THE EDT'S PAST ELECTRONIC CIVIL DISOBEDIENCE ACTIONS HAVE SHOWN IT IS DETERMINED TO PURSUE ITS ANNOUNCED AGENDA. HOWEVER, BASED ON ITS PAST ACTIONS, THE EDT DOES NOT APPEAR TO POSSESS THE SOPHISTICATION AND ORGANIZATION TO POSE A SERIOUS, WELL-COORDINATED CYBER THREAT AT PRESENT. AT THE SAME TIME, ITS POLITICAL AGENDA HAS BEEN SOMEWHAT SUCCESSFUL DUE TO THE MEDIA COVERAGE IT HAS RECEIVED.

5. THIS COMMUNICATION SHOULD NOT BE FURNISHED TO THE MEDIA OR OTHER AGENCIES OUTSIDE THE LAW ENFORCEMENT/U.S. GOVERNMENT COMMUNITY WITHOUT THE PERMISSION OF THE FBI/NIPC. CONTACT POINT FOR THIS COMMUNICATION IS THE [redacted] AT [redacted] b7E

[redacted] OR [redacted]

BT

#0025

NNNN

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/30/1998

To: Atlanta

From: Atlanta
Squad [ ]
Contact: [ ]

Approved By: [ ]

b6
b7C

Drafted By: [ ] :tbf

Case ID #: 288-AT-87255 ~~(Pending)~~

Title: UNKNOWN SUBJECT(S), AKA
ELECTRONIC DISTURBANCE THEATER (EDT)
DEPARTMENT OF DEFENSE (DOD)
CITA - DENIAL OF SERVICE/INTRUSION

Synopsis: Alleged acts of electronic disruption to target the U.S. Army's School of the Americas (SOA).

Details: An entity known as the "Electronic Disturbance Theater", sympathetic to the Zapatista movement, had been calling for civil disobedience actions at the School of Americas on November 22, 1998. This information was posted on the EDT's publicly-accessible web site, www.thing.net/(TILDE) rdom/ecd/November.html. The EDT claims its actions have been prompted by the school's increasing role in training T4E Mexican Military since the January 1, 1994, Zapatista uprising. The EDT is a group consisting of activists who have primarily targeted U.S. and Mexican Government sites in support of Mexico's Zapatista National Liberation Army.

The EDT has a History of carrying out its threats utilizing FloodNet, a denial of service software tool, designed to disrupt access to targeted web sites by flooding the host server with repeated requests for that web page. To accomplish this, FloodNet users simply leave their browsers open, which allows the FloodNet applet to automatically reload a target web page every few seconds. This tool also allows the user to post his own messages on the target web page.

On November 23, 1998, the writer was contacted by New York Case Agent SA [ ] New York file 288-NY-268557 and she advised that EDT's Internet website solicits visitors to participate in coordinated attacks of a computer system chosen by EDT. Participants simply click on the FloodNet icon on the EDT's website at a predetermined and published date

b6
b7C

File will remain on SE. Rotor, SA Columbus, RA. [ ] will be POC for NY & AT.

b6
b7C

SEARCHED ____ INDEXED ____
SERIALIZED ____ FILED ____
DEC 07 1998
FBI - ATLANTA

288-AT-87255-4

and time. This icon then initiates a Java applet which repeatedly reloads files from a victim's computer system at a unusually high rate. This activity, when multiplied by many users, will cause service interruptions and possibly crash the server computer unless early detection is made and countermeasures are implemented. The visitors do not control the destination of the attack, rather it is programed into the applet on the EDT's website.

The EDT claims that it designed the FloodNet program and has attacked computer systems owned by the Government of Mexico, the Department of Defense, and the German Stock Exchange. The New York Office has identified the proprietors of EDT to be New York University Graduate Students located in New York, New York.

On November 22, 1998 an electronic attack was launched against the School of Americas, Fort Benning, Georgia. SA [redacted] of the Columbus RA was contacted and he was put in touch with FBIHQ, [redacted] and New York Case Agent [redacted] The local news reported that Actor Martin Sheen led 2,300 protesters onto Ft. Benning to protest the Army's School of the Americas, and the Army responded by taking them on a ride in military buses to a nearby park and letting the protesters go free without arrest. b6 b7C

In that the New York office has identified the members of the EDT within their division, and all Atlanta leads are at Ft. Benning, Columbus, Georgia, it is recommended that all future leads for Ft. Benning be sent to SA [redacted] of the Columbus RA. Atlanta will continue to keep New York apprised of any new developments.

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 09/14/1999

To: SAC, Atlanta

From: Atlanta
Squad [ ]
Contact: SA [redacted]

Approved By: [redacted] b6 b7C

Drafted By: [redacted]:tbf

Case ID #: 288-AT-87255 (Closed)

Title: UNSUB(S);
ELECTRONIC DISTURBANCE THEATER (edt);
DEPARTMENT OF DEFENSE (DOD);
CITA-DENIAL OF SERVICE/INTRUSION

Synopsis: All investigation concerning the above captioned case has been completed, and it is recommended that the case be administratively closed.

Details: On November 22, 1998, an electronic attack was launched against the School of Americas, Fort Benning, Georgia. An entity known as the ▒Electronic Disturbance Theater▒, sympathetic to the Zapatista movement, had been calling for civil disobedience actions at the School of Americas on November 22, 1998.

The EDT has a history of carrying out its threats utilizing FloodNet, a denial of service software tool, designed to disrupt access to targeted web sites by flooding the host server with repeated requests for that web page.

The Electronic Disturbance Theater is apparently a group of about five activists and they are believed to be New York University Graduate Students located in New York. Based on the above facts, any information concerning the EDT, is being sent to New York.

DMA 17
Close 4 9.24.99
9/22/99

♦♦

288-AT-87255-5